UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,985	08/29/2001	Masahiro Kaminaga	NIT-294	5972

7590 05/01/2006

MATTINGLY, STANGER & MALUR, P.C.
Suite 370
1800 Diagonal Road
Alexandria, VA 22314

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/940,985	KAMINAGA ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) *1-4* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 February 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 03 February 2006. By this response, Claims 5-7 and 11 have been amended. No claims have been added or canceled. Claims 1-4 were previously withdrawn from further consideration as being drawn to a nonelected invention. Claims 5-13 are currently under consideration in the present application.

Response to Arguments

2. Applicant's arguments with respect to claims 11-13 have been considered but are moot in view of the new ground(s) of rejection.

Specification

3. The Examiner thanks Applicant for careful attention to correcting errors in the specification. However, the Examiner notes that the amendment to the paragraph on page 16, beginning on line 2 (noted at pages 2-3 of the present response) makes reference to "An Introduction to the Theory of Cryptography", which appears to be a prior art reference. However, there does not appear to be any further identification for this reference (for example, author(s), publisher, date of publication, etc. as appropriate), nor does it appear that the reference was cited on a received Information Disclosure Statement.

4. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 5 and 6 have been amended to include limitations not described in the specification. Specifically, the claims have been amended to recite transferring data "in order of its bit sequence". There is no written description for such a limitation in the specification. See below regarding the rejection of Claims 5-10 under 35 U.S.C. 112, first paragraph.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 5-10 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contain subject matter that was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, Claims 5 and 6 have been amended to include limitations not described in the specification. Claim 5 now recites transferring one operation unit in the bit pattern of data A or B "in order of its bit sequence". Claim 6 now recites transferring one operation unit of data A or B "in order of its bit sequence".

There is no description of data transfer in order of a bit sequence. Further, it appears that the term "bit sequence" does not appear in the specification. Claims 7-10 are rejected due to their dependence on a rejected base claim.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 5-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 5 recites the limitation "its bit sequence" in lines 7-8, 9-10, 12, and 14 of the claim. It is not clear what the antecedent of "its" is. That is, in lines 7-8, it is not clear whether "its" refers to the operation unit, the bit pattern of data A, data A itself, or the memory; in lines 9-10, it is not clear whether "its" refers to the operation unit, the bit pattern of data B, data B itself, or the memory; in line 12, it is not clear whether "its" refers to the operation unit, the bit pattern of data B, or data B itself; and in line 14, it is not clear whether "its" refers to the operation unit, the bit pattern of data A, or data A itself. This renders the claim indefinite.

Similarly, Claim 6 also recites the limitation "its bit sequence" in lines 7, 8-9, 11, and 13 of the claim. It is not clear what the antecedent of "its" is. This renders the claim indefinite in a similar manner as described above in reference to Claim 5.

Claims 7-10 are rejected due to their dependence on rejected Claim 6.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 11-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Kocher et al, US Patent 6327661 (cited in the previous Office action).

In reference to Claims 11 and 12, Kocher discloses a tamper-resistant processing method including randomly selecting an unprocessed operation unit in data A corresponding to a generated random number, executing an arithmetic operation on the unit of the data A and a corresponding unit of data B, storing the result, and repeating the above steps until the operation has been completed (column 10, line 50-column 13, line 20; noting particularly column 10, lines 57-59, column 12, lines 13-19, and column 13, lines 11-20).

In reference to Claim 13, Kocher further discloses that the arithmetic operation can be one of logical AND, OR, or XOR (see column 12, lines 45-60).

Allowable Subject Matter

11. Claims 5-10 would be allowable if rewritten or amended to overcome the rejections under 35 U.S.C. 112, first and second paragraph, as set forth in this Office action.

12. The following is a statement of reasons for the indication of allowable subject matter:

Claims 5 and 6 are directed to processing methods in which the order of loading two registers is varied for each "operation unit" of two blocks of data before an arithmetic operation is performed on the blocks of data; i.e. it is decided whether the unit of data A is loaded into its respective register before the unit of data B is loaded into its respective register, or whether the unit of data B is loaded before the unit of data A. Although Kocher et al, US Patent 6278783, discloses randomly varying the order in which arithmetic operations are performed on units of two blocks of data, and Kocher et al, US Patent 6327661, discloses randomly permuting the order in which operations are performed on units of data, neither reference by Kocher teaches nor suggests varying the order loading into the registers the units of blocks of data in sequence.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Gressel et al, US Patent 6748410, discloses methods for performing calculations and many techniques for avoiding leakage of data that could be vulnerable to power/current analysis or other side-channel attacks.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER